# Information Operations Newsletter

**Compiled by**: **Mr. Jeff Harley**

**US Army Space and Missile Defense Command**
**Army Forces Strategic Command**
**G39, Information Operations Division**

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion of research in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of the Army, or U.S. Army Strategic Command.

ARSTRAT IO Newsletter on Phi Beta Iota

ARSTRAT IO Newsletter at Joint Training Integration Group for Information Operations (JTIG-IO) - Information Operations (IO) Training Portal

# Table of Contents

Vol. 13, no. 01 (September – October 2012)

## Taliban Using Facebook to Lure Aussie Soldier

By Anthony Deceglie, The Sunday Telegraph, September 09, 2012

TALIBAN insurgents are posing as "attractive women" on Facebook to befriend coalition soldiers and gather intelligence about operations.

Australian soldiers are given pre-deployment briefings about enemies creating fake profiles to spy on troops.

Personnel are also being warned that geo-tagging - a function of many websites that secretly logs the location from where a post is made or a photo is uploaded - is a significant danger.

Family and friends of soldiers are inadvertently jeopardising missions by sharing confidential information online, the report warns.

Three Australian soldiers were this month murdered inside their base, allegedly by an Afghan Army trainee.

The dangers of social media are revealed in a federal government review of social media and defence, which was finalised in March but has not been acted upon, Defence sources say.

The review found an "overt reliance" on privacy settings had led to "a false sense of security" among personnel.

The review warns troops to beware of "fake profiles - media personnel and enemies create fake profiles to gather information. For example, the Taliban have used pictures of attractive women as the front of their Facebook profiles and have befriended soldiers."

Many of the 1577 Defence members surveyed for the review had no awareness of the risk, it said, adding 58 per cent of Defence staff had no social media training.

Surveyed troops said social media open "a whole can of worms when it comes to operational, personnel and physical security".

"Many individuals who use social media are extremely trusting," the review said.

"Most did not recognise that people using fake profiles, perhaps masquerading as school friends, could capture information and movements. Few consider the possibilities of data mining and how patterns of behaviour can be identified over time."

The review recommended education for family and friends on the dangers of sharing details like names, ranks and locations.

Several troops argued for a total social media ban. "I see too many members who post info/pics of themselves which identify ... what unit they belong to and where they are serving," one said.

Security expert Peter Hannay, from Edith Cowan University's school of computer and security science, said geo-tag information "can be data-mined and sold to anybody".

The Department of Defence said it was working on new social media guidelines, to be released by Christmas.

Table of Contents

## Army and Marines Creating Systems for Cyber Fire Support

By John Reed, Foreign Policy, September 10, 2012

The Army and Marine Corps are developing procedures that allow front-line troops to request offensive cyber support the same way they currently request artillery and air support.

For its part, the Army has fielded the Cyber Effects Request Format, or CERF, a system tht allows combatant commands to request cyber operations from U.S. Cyber Command.

"It's an Air Force model that we deliberately seized on about 19 months ago, a close air support model, to develop a process and procedures by which tactical and operational commanders can leverage these fires in support of their operations," said Lt. Col. Jason Bender, chief of fires for Army Cyber Command on August 15. ("Fires" is the military term for discharging weapons. So no, Bender isn't Army Cyber's chief arsonist.)

Requests for cyber fire support will go up through the same chain of command as air or artillery support and will end at cyber operators providing the solutions, according to Bender.

Right now, the CERF allows combatant commanders and operational commanders to request cyber support for their missions. However, the Army would like to expand this so that smaller, tactical level units fighting on the ground can request cyber fire support.

"Just about all the services would like to be able to [provide cyber fire support to tactical level troops], the question right now is, what is a cyber tactical fire," said Bender during a Sept. 7 interview. "Most of the fires that we're doing are at the operational or strategic level of war." Since cyber operations don't have physical boundaries, limiting the effects of cyber fires "to a small tactical area is pretty difficult right now."

However, one of the biggest challenges with providing cyber fire support is making sure that planners throughout the military understand what cyber tools are available to them, how to use those tools, as well as possible unintended effects of a cyber strike (similar to the way military planners must work to avoid civilian casualties from airstrikes).

"It's really no different than most of the operations that we're doing in the way we plan and consider them," said Bender.

"With conventional weapons, it's very easy to say ‵I've got a bridge and I want to deny road traffic or deny a line of communication.' As a weaponeer, I can go look at that bridge, and I've got all these weapons that are available to me and all I've got to do is put six JDAMs [GPS-guided bombs] across the bridge or hit the pylons in a certain way and I'm going to drop the bridge and I'm going to deny that line of communication, that road going across the bridge," said Bender. "That's not always so easy in cyberspace."

Commanders, versed in traditional military weaponry and the effects of those weapons, must know what exactly they want to do from a cyber perspective and understand all the collateral effects of their actions and how they interplay between the cyber and physical domains, according to Bender.

"Consider an unclassified network inside of a ground force headquarters, and we have the ability to infiltrate that network and disrupt their communications on it or do [misleading] message delivery. If we destroy that headquarters building, we also destroy our [cyber] characteristics of the target, so that target ceases to exist in cyberspace," potentially undermining a cyber mission, said Bender.

At the same time, cyber planners must be aware of the needs of ground troops when planning cyber operations, Bender told Killer Apps in a follow-up interview.

To this end, the Army is working to view targets through a holistic lens that takes into account what impact kinetic operations will have on cyber operations and vice versa. Why bomb an enemy into submission when you can simply confuse him into ineptitude for a fraction of the cost?

"Cyber capabilities and effects are instantaneous," said Lt. Gen. Rhett Hernandez, commander of Army Cyber Command on Aug. 16. "However, cyber planning and targeting are resource intensive, our planners and analysts continue to integrate cyber targeting with [military] objectives, the joint fires process, and lethal and non-lethal effects."

In, English, that means that the Army's cyber planners are working to make sure everyone understands how long it can take to plan a cyber mission and how cyber weapons work. Doing so will ensure that commanders know what type of cyber weapons are available to them and how to use them.

Meanwhile, the Marine Corps is also hustling to equip expeditionary fighting groups known as Marine Air Ground Task Forces (MAGTFs) with cyber weaponry to take into battle alongside their rifles, artillery, tanks, helicopters and airplanes.

"The future environment . . . leads us not only to focus on [cyber] vulnerabilities [and opportunities] at the strategic levels, but to create options for the most forward, tactical commanders to use cyber as an important weapon within their quiver," the Marines' top cyber warrior, Lt. Gen. Richard Mills, said on Aug. 15.

"That MAGTF commander at the front end of the spear will have organic, offensive [cyber] capabilities, they will be augmented by fires from [Marine Corps Cyber Command] and from U.S. Cyber Command and, perhaps ultimately, from NSA," added Mills, referring to the National Security Agency, considered one of the most potent cyber fighting organizations in the world.

Mills admitted that his forces used offensive cyber operations to "great impact" in Afghanistan when he commanded all Marines there in 2010.

"I was able to get inside [enemy networks], and affect his command and control and, in fact, defend myself against his almost constant incursions to get inside my [cyber] wire to effect my operations," Mills said on Aug. 15

Table of Contents

# There Goes the Siren of Psy-War

By Shankar Roychowdhury, Asian Age, Sep 04, 2012

Was the violence in Mumbai, Pune, Bengaluru and Hyderabad deliberately engineered at carefully selected targets of strategic importance?

Gulmarg" 1947, "Gibraltar" and "Grand Slam" 1965, "Changez Khan" 1971, and "Badr" 1999 — all these are Pakistani code words for the offensives launched against India during the Indo-Pak wars of those years.

But now India is facing a different, perhaps unique, offensive from Pakistan, for which no code name has been employed as yet. It is a campaign of deniable psychological warfare which targets the very "idea of India" by developing communal fissures within its civil society. This was graphically demonstrated in the chain of events interlinking ethnic violence in Assam, Mumbai and Bengaluru. This is a storm warning the country can ignore only at its own peril.

Pakistan realised quite early that it could never hope to substantially damage India by conventional armed conflict. It changed its strategy, settling for terrorism, low-intensity warfare and psychological operations. It is thus not unimaginable to suggest that the communal violence triggered by the riots in Assam's Kokrajhar district, exploited in Mumbai followed by the exodus of the people of the Northeast from Bengaluru and other southern states was not caused by spontaneous combustion after communal riots, but by deliberate actions with much deeper overall strategic objectives than may be immediately apparent.

It should also not be considered totally far-fetched to assume that the current wave of communally motivated retaliation in Mumbai, Pune and Bengaluru organised by "unknown persons" in the aftermath of the Assam riots, targeting people of north-eastern origin can, in fact, be acts of planned psychological warfare engineered by covert agencies from across the border to destabilise the country. The process of denial commenced the moment "Pakistan" was mentioned and was followed by cursory dismissal by Pakistan of the Indian home minister's rather plaintive complaints, with the characteristic undertones of ridicule which come across in all such interactions, and which India has learnt to put up with.

The communal disturbances that broke out in Mumbai at the conclusion of the mammoth protest meeting of Muslims organised on August 11, 2012, against the backdrop of the violence in faraway Kokrajhar was organised by the Raza Academy, about which nothing much is known, even to the Mumbai Police. This mysterious academy, of course, promptly disclaimed all responsibility for the violence. It claimed that the violence was the work of outsiders even though it was this very meeting which provided the platform for incendiary communal speeches and became the launchpad for the outbreak.

To further inflame passions which rapidly built up at the venue, the events in Assam were even connected with the massacre of Rohingya Muslim community in the Rakhine province of Burma. Matters soon got out of hand as they usually do in these circumstances and, though the Mumbai Police claimed that the rioting had been brought under control within a very short time, it was apparent that there was no prior information or intelligence about the likelihood of such a contingency. As an intelligence failure, the Mumbai riots perhaps ranked on a scale comparable to 26/11, from which no lessons appear to have been learnt. So, too, was the situation in Bengaluru, where police intervention was not as firm and timely as it should have been.

With more information gradually seeping into the public domain, it is now becoming increasingly apparent that the communal violence which raced across India, from Kokrajhar to Mumbai, Bengaluru, Hyderabad, Pune and thence to towns in Uttar Pradesh, were carefully stage-managed by expert manipulation of public perceptions. The tools were gossip and rumours, propagated by doctored images on social media originating in Pakistan. Thus it would not be alarmist to discern an organised campaign of psychological warfare (psy-war), managed with professional expertise and competence by shadowy across-the-border agencies, whose identities are gradually coming to light.

Psychological warfare is still a relatively less-known entity in India. It is directed against the individual as well as collective human psyche and perceptions and is difficult to counter, unless an equally deliberate plan of counter-psychological warfare is developed. This is not a traditional military operational skill, but an esoteric branch of conflict requiring the special expertise of diverse high-calibre professionals not otherwise associated with the military — psychologists, public relations personnel, journalists, media and advertising professionals. These capabilities require substantial enhancement.

There are several significant factors common to the outbreaks in Mumbai, Bengaluru and Hyderabad. To begin with, all three cities are located in the national heartland of information technology, with a large presence of national research facilities, strategic manufacturing and scientific institutes. It is thus intriguing that the fallout of a communal outbreak in the rural environments of Kokrajhar could have such powerful repercussions in Mumbai, the economic capital of the country, and Pune, Hyderabad and Bengaluru, all significant centres of high-technology research and manufacturing, many related to sensitive key areas of defence, including missiles, guided weapons and aerospace.

Seen in this context, was the violence in Mumbai, Pune, Bengaluru and Hyderabad deliberately engineered at carefully selected targets of strategic importance? Have the Kokrajhar riots, tragic and deplorable as they undoubtedly are, been seized upon by hostile agencies as a window of opportunity to launch a larger and more deliberate plan to disrupt India's strategic potential and create some degree of chaos in the country? Official agencies involved with internal security psychological operations and counter-intelligence should be looking for answers to these questions.

There are other concerns too, about short-sighted political manoeuvres developing around Assam, Mumbai and Bengaluru. The consequences can be extremely dangerous for the safety and security of the nation. It is, therefore, a matter of urgency that the wider ramifications of any Kokrajhar-Mumbai-Bengaluru linkage should be rapidly investigated and brought to light.

Table of Contents

## Get Ready For Next Stage of Electronic Warfare: Expert

From WebIndia123.com, Sep 8 2012

Electronic Warfare (EW), in which India has gained good expertise, will now lead to the next stage -- the 'Electro Magnetic Spectrum Warfare' and the experts should get ready for it, an expert today said. Speaking after the awards ceremony organised by the Indian Chapter of 'Association of Old Crows' (AOC), a professional organisation specialising in EW, DRDO Chief Controller (ECS and LIC) S S Sundaram said the development of EW was evolving and the country was witnessing the fourth generation of scientists who fittingly received awards for their efforts by AOC today. 'With warfare now slated to be fought in space as well, EW has made way to Electro Magnetic Spectrum Warfare. But India does not have the capacity to excel in this field yet and we need to build it. AOC, with the veteran defence experts in its ranks, should step in and coordinate with DRDO, defence forces and the private sector involved in production of niche defence technology,' he said. He said with satellite-based warfare systems coming in, there would be lot of opportunities for the defence production sector in the country as there will be vast requirements in the space-based EW.

Table of Contents

## Coming Soon On Demand: Cyber Weapons

Posted By John Reed, Foreign Policy, September 5, 2012

Air Force cyber planners have developed a new approach to buying cyber weapons that they hope will enable them to keep pace with threats in a field where technological advances happen in days, or even hours.

Last month, the Air Force Research Laboratory (AFRL) gave six firms contracts valued at up to $300 million under a program called Agile Cyber Technologies (ACT), which will essentially keep these companies on retainer to provide cyber weapons on-demand under a form of contracting known as Indefinite Delivery-Indefinite Quantity (IDIQ).

The ACT program will be used to quickly develop cyber weapons that do everything from defending Air Force networks to spying on enemy networks and conducting offensive cyber attacks, according to the service's draft request for proposal for the program.

Basically, if the Air Force sees the need for a new cyber weapon, it can immediately tap one of its contractors to develop and field the technology quickly rather than go through an infamous military procurement system that can take anywhere from months (for small buys under "rapid equipping" programs) to decades to field a new weapon system.

CACI, Assured Information Security Inc., L-3 Communications, Radiance Technologies, ITT Exelis, and Global Infotek have all been given contracts through 2018.

While the dollar amount of the ACT contract may relatively modest by Pentagon standards, the program is important because it could pave the way for how the Air Force and the rest of DoD stays ahead of the tech curve in the cyber realm. No more bulky acquisition contracts for single types of weapons, just one retainer fee to continually develop new weapons.

"Government is moving more to IDIQ contracts to respond faster to new technologies and respond to the fast evolving threats," Per Beith, director of information security solutions for Boeing, another company that is moving aggressively into the cyber security market, told Killer Apps. "Some of our customers have discussed looking at implementing commercial models like buying from an ‘app store' that puts the burden of development risk on the contractor instead of the government."

"There is a driving need for rapid cyber development solutions, and AFRL's ACT effort is the type of flexible and innovative contract that meets that need," said Dr. Ray Emami, president of Global Infotek in a statement about the contract.

This comes as the Pentagon's overall plans to speed the purchase of cyber technology have hit a rough patch, with DOD officials worrying that the senior-level purchasing committee they are setting up to quickly buy cyber weapons -- dubbed the  Cyber Investment Management Board --  will, ironically, slow the process due to the simple fact that it is another Pentagon bureaucracy made up of top DOD officials whose time and attention are already spread thin.

Table of Contents

## Iran Blocks Access to Gmail

AFP, 24 Sep 2012

TEHRAN — Iran blocked access to Google's popular and relatively secure Gmail service Monday amid first steps by the Islamic republic to establish a walled-off national intranet separate from the worldwide Internet.

Access to Google's search page (www.google.com) was also restricted to its unsecured version, web users in Iran found. Attempts to access it using a secure protocol (https://www.google.com) were also blocked.

The curbs were announced in a mobile phone text message quoting Abdolsamad Khoramabadi, an adviser to Iran's public prosecutor's office and the secretary of an official group tasked with detecting Internet content deemed illegal.

"Due to the repeated demands of the people, Google and Gmail will be filtered nationwide. They will remain filtered until further notice," the message read.

Google's own website tracking country-by-country access to its services did not immediately reflect the blocks (www.google.com/transparencyreport/traffic/?r=IR&l=GMAIL&csd=1230796800000&ced=1348461000000).

But several residents in Tehran told AFP they were unable to get into their Gmail accounts unless they used VPN (virtual private network) software.

VPNs are commonly used by tech-savvy Iranians to get around extensive online censorship, though bandwidth of connections through the software is routinely strangled and occasionally even cut entirely.

Gmail is used by many Iranian businessmen to communicate and exchange documents with foreign companies. Iran's economy is suffering under Western sanctions that have cut oil exports and made trade more difficult.

Iranian authorities previously and temporarily cut access to Google and Gmail in February, ahead of March parliamentary elections.

Google's popular YouTube video-sharing site has been continually censored since mid-2009, following protests and opposition claims of vote fraud in the wake of elections that returned President Mahmoud Ahmadinejad to power.

Other social networking sites, such as Facebook and Twitter, are also routinely blocked.

Iran is working on rolling out its national intranet that it says will be clean of un-Islamic content. Officials claim it will be faster and more secure, even though users' data will be more easily subject to monitoring.

Despite fears by Iranians that the new intranet would supplant the Internet, Mohammad Soleimani, a lawmaker heading a parliamentary communication committee, was quoted last week by the ISNA news agency as saying that "the establishment of the 'National Internet' will not cut access to the Internet."

He added: "Cutting access to the Internet is not possible at all, because it would amount to imposing sanctions on ourselves, which would not be logical. However, the filtering will remain in place."

Table of Contents

## Keeping Nukes Safe from Cyber Attack

By John Reed, Foreign Policy, September 25, 2012

In the wake of a 2010 incident in which the Air Force lost contact with 50 intercontinental ballistic missiles, the service is figuring out how to protect its command-and-control systems from cyber attack -- a nonexistent threat when the missiles were designed decades ago.

"Our ability to keep our networks assured and protected and not vulnerable is really important, it's something we have looked at hard," Maj. Gen. William Chambers, head of Air Force Global Strike Command's nuclear deterrence shop, told Killer Apps during a Sept. 18 interview. "It's something that we build into all of our new nuclear weapons systems so that they remain cyber-secure."

Global Strike Command manages U.S. land-based nuclear ICBMs and air-launched nuclear cruise missiles and bombs.

Protecting what are arguably the nation's most important military assets from cyber attack, and avoiding the terrifying scenario of an enemy feeding incorrect information into the nuclear command-and-control networks "seized" Air Force officials after they lost contact with a field of 50 Minuteman III ICBMs at FE Warren Air Force Base in Wyoming for an hour in late 2010, according to Chambers.

"It's really important. It's a problem that about a year ago we were seized with. We have done some pretty comprehensive studies of the cyber-state of our ICBM force. We are confident in it," said Chambers. "There was an issue: we had a temporary interruption in our ability to monitor one of our missile squadrons back in the fall of 2010. That produced a need to take a comprehensive look at the entire system. It took a year to do that study, and we're confident that the system is good, but as we upgrade it, modernize it, integrate it, we've got to really pay attention to" protecting nuclear command-and-control information.

While Chambers didn't go into specifics of how Global Strike Command will protect its nuclear command-and-control networks from cyber attack, he did say that it is working to harden its networks against intrusion and the manipulation of nuclear command-and-control information and to increase backup communications abilities.

Chambers added that the Minuteman III ICBM command systems, designed in the 1960s and 1970s, are incredibly robust. "ICBM-wise we have a very secure system."

A Boeing official later told Killer Apps that while it is looking at upgrading the ancient technology used in parts of the Minuteman command networks, that technology is safe from hacking. Boeing is on contract with the Air Force to maintain the 1970s-vintage Minuteman III fleet and is helping the service keep the missiles in service through the 2030s.

"Our C2 [command-and-control] system for Minuteman is a very old system. There's a network called the HICS [hardened intersite cable system] network, and it's [made of] copper wire, and it's limited in bandwidth," said Peggy Morse, director of Boeing's strategic missiles systems programs, told Killer Apps on Sept. 18.  While it's old, "it's very secure," she added.

Still, "as we look at different C2 systems and ways to move data about in the field, information assurance is a big deal there, and the security requirements are going to drive the solutions that we look at," said Morse. The company is also working to modernize the actual cryptographic devices used to encrypt and decipher launch codes for nuclear missiles.

Bruce Blair, a former Minuteman III launch-control officer and co-founder of the Global Zero movement to eliminate nuclear weapons, describes several ways the ICBMs' aging command-and-control technology are vulnerable to hacking.

Both the missile silos' radio receivers, which are designed to read messages from the flying command posts that would be used to launch the missiles in the event that land-based command centers have been destroyed, and the HICS cables are vulnerable, according to Blair.

"In the case of Minuteman, there are...potential entry points into the supposed fire-walled command and control system," Blair told Killer Apps in a Sept 25 email. "One of them is the radio antenna at the unmanned missile silos designed to allow airborne launch control centers to inject the three short signal bursts [telling the missiles to identify their targets, arm, and launch] in the event of a breakdown in the local underground command post system (for instance, their destruction by enemy nuclear missiles)."

If hackers were able to take over this antenna, "this entry point could provide access under a range of circumstances such as the loss of control experienced at FE Warren in a squadron of 50 missiles . . .  or such as illicit actions taken by an ‛insider' agent," added Blair.

"Another [vulnerability] are the thousands of cables that run 6-feet underground interconnecting all of the missile silos with all of the launch control centers in a given squadron. It's possible to imagine outside parties surreptitiously tapping into one cable at one location or another, and thereby gaining access to the actual conduits that control and target, enable, and fire the missiles."

Still, doing so would require knowing exactly where the cables are and avoiding security details.

Chambers did not comment on the command systems for the service's air-launched nuclear cruise missiles and B-61 tactical nuclear bombs.

A key part of protecting nuclear weapons from cyber attack as they are modernized and upgraded is making sure that the supply chain for nuclear weapons electronics is secure -- a problem that has plagued the Defense Department for years.

"We are continuing to study the cyber assurance aspect of the supply chain that supports our nuclear weapons systems," said Chambers. "That work is underway and we're taking steps to mitigate and close off any vulnerabilities."

This effort is focused on making sure that Defense Department officials know exactly where the electronic chips and other components used in nuclear command and control come from and how they are produced.

"That's not just our problem, that's a national problem," added Chambers, referring to the fact that the entire DoD is concerned about counterfeit electronic parts making their way into its supply chains. Such parts are at best, potentially unreliable and at worst could be infected with malware aimed at U.S. military gear

Table of Contents

## Cultural Battlegrounds: Why Culture Matters In Global War on Terror

By Dr. William L. Dulaney, Air Force Culture and Language Center, 9/25/2012

9/25/2012 - MAXWELL AIR FORCE BASE, Ala. (AFNS) -- In every culture, there exists the possibility of a mob of people that could be easily compelled to action by those who know how. Understanding culture, for the military professional, should be thought of as the art and science of understanding cause and effect in social contexts.

In operational contexts, culture is human terrain; just as real as the ground on which we fight, the airspace we own and the seas we dominate. Culture subsumes, among so much else, a people's morals, values and ethics -- what is beautiful, right and wrong; what people will or will not fight and die for. These are all aspects of culture that military professionals need to understand to be successful in 21st Century warfare.

Why worry about what is beautiful? Military information support to operations cannot produce effective media and/or conduct psychological operations without a working knowledge of what certain people regard as pleasing to the eye, ear or heart.

Understanding what people consider right or wrong is as important to the private on his first foot patrol through an Afghan village as it is to the four-star general who makes a speech to another nation on international television.

The knowledge of what people are willing to fight and die for should be obvious. Sadly, it is not. Evidence is clear that the spate of Green-on-Blue shootings in Afghanistan is overwhelmingly caused by cultural transgressions. From refusing to urinate in private to condemnations of the Qur'an, we as a military seem not to understand that we sometimes cause our own problems.

Military professionals must, of necessity, not succumb to flimsy explanations, such as those bandied about on television, radio and internet news sources, that "those" people are just "crazies." Sure, fanatics exist in the form of extremists all around the globe. Many of them are lobbing Molotov cocktails, rocks and RPGs at our embassies and consulates across the north of Africa as I write this. But one must ask him or herself: "Which is more likely?" An entire culture of people is crazy enough to be incited to violence by a poorly produced video clip downloaded from the Internet. Or, there are a few - maybe only one - individuals or organizations behind the violence.

Experience has shown that the latter is usually the case. One example is a band of bad actors that understand a culture so well that all they need do is search the Internet for the most effective stimulus to create a predetermined effect on the anniversary of the 9/11 attacks.

Leaders of extremist, Islamist and illicit organizations understand well that culture is a fire burning in the heart of every human. All one needs to do to make that fire erupt into action is fan the flames just a little. And then sit back from a safe distance and watch. Watch as their small efforts spread across a region or even a continent. Watch as we Americans continue to try and explain what is happening while wearing what can only be described as blinders of ethnocentrism. Watch as we lose more American lives and treasure fighting an enemy that is overwhelmingly outmatched on every single plane of warfare save one: the human terrain.

So the challenge seems clear: military leaders of all ranks must strive to cleave the extraneous information away from the actual causes of deadly effects. To understand that it is impossible to fight an idea or ideology, but very possible to target our awesome military might on the specific bad actors perverting ideas and ideologies. To bring the fight to the few who are manipulating the many.

Table of Contents

## Cyberwarfare and Combined Arms

From Information Dissemination blog, September 16, 2012

John Reed had an interesting overview of the Army and Marines' effort to create a "cyber fire support" process in last week's FP National Security. Most of interest to the Information Dissemination audience is the Marines' attempt to put cyber within the MAGTF construct:

> Meanwhile, the Marine Corps is also hustling to equip expeditionary fighting groups known as Marine Air Ground Task Forces (MAGTFs) with cyber weaponry to take into battle alongside their rifles, artillery, tanks, helicopters and airplanes. "The future environment . . . leads us not only to focus on [cyber] vulnerabilities [and opportunities] at the strategic levels, but to create options for the most forward, tactical commanders to use cyber as an important weapon within their quiver," the Marines' top cyber warrior, Lt. Gen. Richard Mills, said on Aug. 15. That MAGTF commander at the front end of the spear will have organic, offensive [cyber] capabilities, they will be augmented by fires from [Marine Corps Cyber Command] and from U.S. Cyber Command and, perhaps ultimately, from NSA," added Mills, referring to the National Security Agency, considered one of the most potent cyber fighting organizations in the world.

In the 1990s, most discussion about the broader field of information warfare was couched within the framework of the Revolution in Military Affairs (RMA). Either it was about using the network to create Dominant Battlespace Knowledge (one of many concepts that seemed misplaced in retrospect) or stand-alone strategic information warfare to disable the enemy's system of systems. Very little, if any, cyber discussion was couched within a combined arms construct. Today, strategic and standalone information warfare against vulnerable rear areas is still the most prominent area of the cyber discussion. Unfortunately, there hasn't really been very much conceptual advance in that area. Many audiences are unaware of formative cases such as Solar Sunrise or Moonlight Maze and the problems they revealed with US cyber defenses.

Real-world experience and the need to bring capabilities within existing organizational frameworks is motivating a combined-arms approach. There are, however, some risks involved. First, the phrase "weapon" understates the variability of effects that the current generation of cyber-weapons generate as well as the diminishing financial and strategic returns inherent in their current form. As James Hasik notes, precision-guided weapons actually are economical when compared to the cost of deploying cheaper but more numerous "dumb" bombs and delivery vehicles but cyber weapons do not necessarily offer similar savings. The target intelligence, testing demands, legal concerns, shortage of cyber operators, and hat-tipping effects (once used, an vulnerability is exposed to the enemy) inherent in the weapons suggest complications for integrating this sort of weapon into a standard combined arms matrix. That is, if the matrix conceives cyber weapons as somehow equivalent to disembodied field artillery pieces waiting in the ether for grid coordinates. Certainly making things go boom matters, but it is not the only means to an end.

One of the dominant conceptual problems involved in thinking about cyber weapons is also the focus on weapon instead of effect. There were many faults with Effects-Based Operations (EBO), but it at least looked at the problem from the framework of linking targeting method to the type of desired effect rather than trying to figure out what effect was necessary to make a given weapon useful. Thinking about cyber solely from the perspective of the electromagnetic network--and kinetic actions to damage it--is part of the problem. One encouraging sign in Reed's article is precisely a focus on blending different kinds of tools together to precisely achieve a cumulative effect. There are a variety of ways within the broader array of cyber capabilities to achieve effects, and too little thinking about what weapons and attack vectors might match them.

As Sam Liles observed, the common link between what he dubs all three "generations" of cyber warfare is the command and control-centric style of warfighting that originated in the late 19th century. Integrated communications networks is a major part of what enabled the large distributed operations possible on both land and sea that is characteristic of modern warfare. But command and control should not be confused with the technical network. Rather, an institution like the Prusso-German General Staff was a human network that, while built around telegraphic information networks, can be regarded as than more than simply just a electromagnetic superstructure. It might best be considered what Tim Stevens has called a "sociotechnical assemblage" of humans and machines. Human networks constitute a formidable weak link that can be leveraged to compromise technical systems.

If, say, the British or the French had thought about information warfare from our present-day framework, operations against telegraphic networks alone would have been a poor use of their resources. That is why the World War II double-cross system, which gave Britain control over the entire German network of secret agents, was probably more effective than a hypothetical attempt to damage German telecommunications infrastructure at blinding and disrupting Berlin's command and control systems. John Hamre's chief insight about Moonlight Maze was precisely that the infiltration exploited the open norms of the civilian research networks associated with the Department of Defense to compromise it. If this sounds familiar, it also is the method that the Taliban may have used to strike Camp Bastion this weekend. While the base's defenses were thought to be impregnable, the attackers likely exploited a variety of human network vectors that counterintelligence planners may have overlooked. Liles' judgment is that the next generation of cyber weapons will target the entire sociotechnical assemblage, and use advanced computational tools to reveal a system's various fault lines and target it with follow-on weapons customized for purpose.

All of this is a bit of a roundabout way of saying that putting a cyber capability within the framework of combined arms will take a better conceptual lens than imagining digital rifles or mortars. The problem it poses for the American way of warfare is that it puts a premium on a kind of thinking about effects and targeting that runs counter to the instinct of turning battles into engineering equations and thinking about machines over people and the social systems they create. What the Army and Marines are doing is definitely a step forward. The question is how it will be realized--and whether it will avoid or repeat some of the past conceptual errors in how we think about incorporating cyber into military's toolbox.

Table of Contents

## U.S. Military Overestimates Value of Offensive Cyberweapons, Expert Says

By Yasmin Tadjdeh, National Defense Magazine, 13 Sep 2012

Efforts by the U.S. military to develop offensive cyberweapons will be futile unless better technologies are developed to identify the perpetrators of a computer network attack, experts said Sept. 13.

"In general, the notion that you can preempt a cyber-attack by using offensive methods is greatly exaggerated," said Martin Libicki, senior management scientist at RAND Corp.

One of the biggest obstacles to fighting back after a cyber-attack is attribution, Libicki said during a cybersecurity conference at the National Press Club, in Washington, D.C.

Another concern is that there can be misinterpretation following an attack, Vincent Manzo, analyst at the National Defense University's Center for Strategic Research said.

In order to stop cyber-attacks, better deterrents are needed, he said.

The predominantly used deterrent currently available is the judicial system, and not traditional military force, Libicki said.

"We think of deterrents as traditionally being reserved for … things that look like acts of war," Libicki said. "Generally speaking, it would be historically unprecedented to respond to espionage with violence or the use of force."

Military leaders have spoken about their attempts to develop offensive cyber weapons as means to deter or respond to attacks. "I tend to be skeptical about cyber deterrents," Libicki said. "I'm not saying we should never hit back, but I would need a lot more indication that a threat to hit back would be all that useful," Libicki said. "It does no good to threaten that if Al-Qaida takes down the American power supply that we'll take down Al-Qaida's power supply, because they don't have a power supply to take down."

With nuclear weapons, deterrence worked because countries were so horrified at the consequences, Libicki said.

"One of the reasons that nuclear deterrents worked was because we never had to make good on that threat. The consequence of being hit with a nuclear weapon were so awful to contemplate that nobody not only wanted to get hit by a nuclear weapon, but they didn't even want to get 10 steps within getting hit with a nuclear weapon," said Libicki.

With the technology that is currently available, the U.S. government's ability to offensively thwart an attack needs work, he said.

Lt. Gen. Michael Basla, vice commander of Air Force Space Command, said at the Cyber 1.2 conference in April that offensive cyber operations are far down a list of nine missions that the command must carry out. While he did not divulge too many details, he listed "deployable cyber-attack system" and "network attack system" as two programs the command was working on.

Libisky also cautioned that hacker attacks on U.S. critical infrastructure may not be as big a risk as government and industry prognosticators have predicted, Libiski noted.

“Something that can take down a poorly defended system in one place may have absolutely no effect on a well defended system somewhere else. It is for this reason that we can only speculate about what a cyber-attack will be,” said Libiski. “[But] it’s a real stretch to say any terrorist could take down a power plant in this country.”

Table of Contents

## U.S. Sets Sights on Iran for Its First Official Cyberwar Campaign

By Constantine von Hoffman, CIO, 16 Oct 2012

The United States is preparing to launch its first officially-acknowledged cyberwar, and the target will almost certainly be Iran.

This war, like another campaign in the same neighborhood, will be based on intelligence only the reigning U.S. Administration has seen and will happen without public approval. Woo and/or hoo.

U.S. Secretary of Defense Leon Panetta said last week that the country is preparing to take pre-emptive action if a serious cyberattack is imminent. In case you had any doubts about how he defines imminent, he also said the United States was at risk of a “cyber-Pearl Harbor.”¬

And, in case that rhetorical flourish wasn’t enough, Leon added, "A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11.” It’s a shame he left out the sinking of the USS Maine.

Panetta added stuff about how U.S. intelligence showed "foreign actors" were targeting control systems for utilities, industry and transport. The actors are also apparently creating advanced tools to subvert key computer-control systems and wreak havoc. No word yet on any cream-frosted yellow-cake uranium, though.

The next day, as if on cue (and it was), The New York Times posted a story with the headline “U.S. Suspects Iran Was Behind a Wave of Cyberattacks.” Lord knows if it’s in the NYT it’s got to be true. Well, except for the last time the government was ginning up an excuse for war.

So is this a well-orchestrated PR campaign by the Administration? Clearly.

Do they have the intelligence proving what they claim? Certainly there are a lot third party reports of Iran doing nasty things, but certainty in the cyber world comes only when you have hard drives in hand.

Or if you're the U.S., according to Panetta: "Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests."

Despite this assurance, the fact is that I have no idea if Iran is doing all that they’re accused of. Neither do you, and that’s a problem.

It’s easy to say that in this case it’s just a cyberwar, so why get so worried? We aren’t putting boots on the ground or manned aircraft overhead, so we’re not putting our own people at risk, right?. For the sake of discussion I will put aside the argument that Iranians are people, too.

First, there’s the principle of the thing.

It’s been 73 years since the last time the U.S. declared and initiated war on a nation. In that time we’ve been involved in five major conflicts and Lord knows how many “minor” ones. (Who can keep count? There’s been at least six in Central America alone.) It is now taken for granted that the President can send U.S. troops into combat for any length of time without needing as much as a nod and a wink from the rest of the American public.

In Korea and the first Iraq war the physical evidence for the casus belli was pretty clear. In Vietnam, we invented the Tonkin Gulf Incident, and in Iraq and Afghanistan we didn’t even bother with that much.

It would be nice if we, the people, were consulted in some way, shape or form before the nation takes military action that isn’t emergency action. Just a thought.

The other issue that always needs to be remembered: In war there is no sure thing. The friction of battle changes plans and outcomes. As we have seen in Iran, even if you win the war easily you can still lose the peace.

But really, what am I getting so concerned about? It’s just a cyberwar. What could possibly go wrong?

"Every gun that is made, every warship launched, every rocket fired signifies in the final sense, a theft from those who hunger and are not fed, those who are cold and are not clothed.  This world in arms is not spending money alone.  It is spending the sweat of its laborers, the genius of its scientists, the hopes of its children.  This is not a way of life at all in any true sense.  Under the clouds of war, it is humanity hanging on a cross of iron."  - Dwight D. Eisenhower, 1953

Table of Contents

# The Cyber Debate Goes Public

By Marc Ambinder, the Week, October 1, 2012

In the parlance of the government, the powerful Gen. Keith Alexander is a "dual-hat."

As director of the National Security Agency, which collects intelligence and keeps and breaks codes, he must operate under the rules of Title 50 of the U.S. code. As the head of the United States Cyber Command (USCYBERCOM), he simply puts on a different hat: Title 10 of the U.S. code, which proscribes conduct for military operations, is his guide.

This germ of a lesson in bureaucratic descriptionaring is a lot more important than it might seem. Alexander is the nation's chief defender of cyberspace, its chief collector of information about cyber threats, and its chief wager of cyberwarfare.

Consider a recent report that Chinese hackers had compromised the White House Military Office's communications systems. WHMO secures communications for the president, runs continuity of government programs, and ensures the integrity of the chain of authorities that allow human beings to launch nuclear weapons. The report alleged that the nuclear command and control (NC2) systems themselves had been compromised; that's not true. WHMO's unclassified email network was hacked; the NC2 systems haven't been touched. But let's say that somehow, China, or someone else, did manage to hack into one of the systems that transmits Emergency Action Messages to, say, strategic nuclear submarines, and a spoof message is somehow transmitted. The U.S. considers any breach of these systems to be an act of war.

Under authorities granted to him by Congress last year, Alexander "has the capability, and upon direction by the president may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests, subject to — (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. 1541 et seq.)." That ought to make you gulp a bit.

"Offensive cyberspace operations" to "defend our Nation, Allies, and interests" covers quite a large territory. Is there anything remotely national-security-ish that isn't permitted by that language?

What Americans know about cyberwarfare is unclear. We read about efforts to hack into military systems; we read about intelligence operations meant to sabotage Iranian centrifuges (a clear national security priority if there was one). More prosaically, many of us are the victim of a minor cyber crimes; not a war, per se; but most of us can get our credit problems made whole or our money back. We read a lot about large breaches of privacy, some of them even state-sponsored. (Google informed me and some other journalists and national security experts that China — a "state sponsor," it said — was trying to break into our email accounts. Hand-wringers in the government worry that, short of a major "kinetic," i.e., death-causing cyber incident, citizens are content to live with this "death by a thousand cuts" approach. The pain of cyber crime is just too distributed for most of us to care, or to alter our cyber hygiene, or to demand that the companies we patronize do the same. This is one reason why cyber legislation stalled in Congress last year, whatever it merits. There just wasn't enough public pressure, or interest, to move it along, despite the herculean lobbying efforts of some of the most powerful forces in government.

One major reason why the public doesn't talk a lot about the way our country might engage an enemy in the cyber is this tangle of Title 10/Title 50 authorities and all the equities that secret-keepers have in keeping the rules fuzzy and flexible. That is why it is significant when Gen. Alexander and others agree to talk about cyberwar in public, and especially when they agree to talk about talking about cyberwar.

Consider Alexander's last few months. There hasn't been a single major think tank whose cyber crime panel he has not graced.  There he was, in July, talking about cyber threats at the American Enterprise Institute. Later that month, he was in the rarefied air at Aspen, telling a security forum that American cyber defenses were about a "3" on a scale of 1 to 10. Alexander spoke to hacker conventions in August. This week alone, he's at the Woodrow Wilson Center and the U.S. Chamber of Commerce.

Because of Congress's inability to pass modern cyber legislation, the White House will soon issue an order spelling out what authority the executive branch claims in the cyber realm. Reportedly, it will contain the rudiments of an information-sharing procedure for the government and the private sector, and will direct the Department of Homeland Security to design a semi-voluntary system for private companies that do business with critical infrastructure. Already, the Department of Defense requires contractors who do critical work to meet top standards.

The issues Alexander brings up are difficult, and attempts to summarize the sides in this complex debate are inevitably going to be glib. But here's a cheer to Alexander for his commitment to talking about the threat. If the director of the NSA wants to lead the way, by all means, let him. It's up to everyone involved, including the private sector, the White House, civil libertarians, and the media, to follow, and to nurture a robust public discussion. Too much is at stake, including money, privacy, and even the integrity of our laws, to let this subject disappear into the ether.

Table of Contents

## Growing Chinese Telecoms Threaten US Security

By Michael Hoffman, Military.com, Oct 04, 2012

Congress and the Pentagon have set their sights on two Chinese telecommunications giants as dangerous potential threats to national security as their wildly popular cell phones start to infiltrate the American market.

U.S. military leaders have listed cyber attacks as a top national threat with the Defense Department, FBI and National Security Agency trying to keep up with the rapidly maturing technological threats facing the government.

The Defense Department sustains more than a 10 million cyber attacks per day. The White House sustained and repelled a serious enough attack Monday that administration officials acknowledged the risk it posed although it didn’t provide details.

Attacks don’t have to infiltrate nuclear missile bunkers or submarine messaging codes to bring a country to its knees. Digital technology penetrates most of American culture. Cell phones lead the way as these tiny computers dictate most Americans’ schedules, communications and even banking.

This dependence on cellular networks has drawn the attention of the U.S. military as Chinese telecommunications firms have grown into global powers. Huawei Technologies Co. Ltd leads the way as it has grown into the world’s largest telecommunications supplier, recently surpassing Ericsson.

What concerns U.S. authorities are the close connections Huawei maintains with the Chinese government and People’s Liberation Army. One report estimates the Chinese government has access to about 80 percent of the world’s communications through their domestic telecommunications corporations.

The House Intelligence Committee has launched an investigation into Huawei and ZTE Corporation, another telecommunications giant, to probe those companies’ Chinese government connections and decide if they can safely operate in the U.S.

Australian politicians have already decided that Huawei poses too severe a threat and has banned the telecommunications corporation from doing business in Australia.

The ranking member of the House Intelligence Committee flew to Hong Kong in June to meet with the leadership of Huawei and ZTE. U.S. Rep. C.A. Dutch Ruppersberger, D-Md., took the roughly 17-hour flight to deliver a message: The U.S. will not allow Huawei and ZTE to serve as espionage arms to the Chinese government inside American borders.

“The whole purpose of the investigation is to determine whether China or other countries had the ability to engage in our networks and control our networks and steal information from our networks by having some of their companies doing business in the United States,” Ruppersberger said.

He takes cyber threats seriously saying the country doesn’t realize just how vulnerable it is to a massive attack.

“Cyber attacks are one of the most serious threats to our country, not only to our domestic business, but also our national security,” he said.

A high level U.S. federal report released in March cited the Chinese military’s access to civilian telecommunications hardware as a major concern. Huawei’s founder is a former PLA soldier. His army background has caused much of the hand wringing over his company’s connections to China’s military.

“This close relationship between some of China’s — and the world’s — largest telecommunications hardware manufacturers creates a potential vector for state sponsored or state directed penetrations of the supply chains for microelectronics supporting U.S. military, civilian government, and high value civilian industry such as defense and telecommunications,” stated a report by the U.S.-China Economic and Security Review Commission.

The report’s authors described how the penetration of a telecommunications supply line could cause a “catastrophic failure of select systems and networks supporting critical infrastructure for national security of public safety.”

China’s military has made major strides in its cyber capabilities as the U.S. still struggles to figure out how cyber attacks fit into its military’s architecture. Service leaders still question what their responsibilities entail outside protecting their own networks.

The commission found that China’s “capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict.” Authors of the report expect China’s initial response to a conflict with the U.S. to include a cyber attack against American logistics and intelligence networks.

Huawei’s founder told Ruppersberger their company poses no threat to Americans’ privacy or security. The congressman described his meeting with Ren Zhengfei, Huawei’s founder, similar to a deposition in which he tried to collect information for the House investigation into the company. However he did deliver a warning to Zhengfei.

“I said we in the United States are [in favor of] free enterprise but we also have to protect our citizens and we are very concerned about Chinese cyber-attacking our businesses and it has to stop. [The] more active China is in cyber attacking the United States, the more it’s going to hurt your ability to do business in our country,” Ruppersberger said he told Zhengfei.

Officials from the U.S.-China Economic and Security Review Commission focused Huawei’s relationship with the Chinese government. They found numerous examples of Huawei working together with China to include training events with military personnel.

“Huawei may also be involved in supporting PLA active-duty units with short term training in networking design and construction, possibly supporting the military region command system with technical experts and “train-the-trainer” program” the commission found.

Huawei works closely with the Chinese military on research and development projects either “directly as a vendor or indirectly as a research collaborator,” which weakens “claims by Huawei’s leadership that it maintains no ties with the Chinese government or the military,” the commission found.

Much like the U.S., the British are closely monitoring how these Chinese telecommunications networks have infiltrated their domestic market. Huawei has tried to assuage British fears by establishing security teams inside British borders near Cheltenham.

The British military has its own doubts. Leadership fears that the British communications networks have already become too dependent on the Chinese telecommunications giants. Huawei equipment runs nearly half of the British communications network, said Ross Anderson, a professor at University of Cambridge Computer Laboratory.

Anderson described how a telecommunications company like Huawei doesn’t necessarily need to install backdoor mechanisms to pose a threat. The company can implant a virus into the regular updates a network requires.

Inside the tens of millions of lines of code that run those updates, a company can hide a targeted attack for espionage purposes, Anderson said.

Huawei officials have approached Anderson to learn about the global communications networks. Anderson has stopped his meetings with Huawei after he got tired of the one-way relationship the company maintained with the Cambridge professor.

“I found them to be an information sponge. [Huawei officials] always want to absorb information but never want to provide information,” Anderson said.

He wrote a report for the European National Security Agency that focused on the importance of global routers and their control over the global communications node. Huawei controls about 20 to 30 percent of those routers, Anderson estimated.

Control of those routers could allow Huawei to shut down much of the world’s internet access and communication network “for a few days”-- paralyzing international marketplaces and militaries.

“[Leadership] has nightmares of China being able to shut down communications in a national security crisis,” Anderson said.

Table of Contents

# Taliban Demands Unbiased Coverage of Its Attempted Murder of a 14-Year-Old Girl

By John Hudson, the Atlantic Wire, Oct 17, 2012

Pakistan's Taliban insurgency faces a spate of bad press in mainstream Pakistani outlets related to the jihadists' failed assassination attempt of Malala Yousafzai, a young blogger who dared protest the Taliban's ban on educating girls. Now the Taliban are plotting terror strikes on TV stations and other media organizations, but local newspapers refuse to stay silent.

The first report of these plots were surfaced by an urdu-language reporter on Saturday, who uncovered a special directive by the chief of the banned Tahreek-i-Taliban Pakistan (TTP) Hakimullah Mehsud. As local newspaper Dawn reported, "Mehsud directed his subordinate to target the offices of media organisations in Karachi, Lahore, Rawalpindi, Islamabad and in other cities of the country especially those media organisations and media personalities who were denouncing TTP after attack on child activist Malala Yousufzai." In response, the Interior Ministry has beefed up security near media organizations. But the Taliban are still whining.

Yesterday, local paper The News International gave voice to the Taliban's pathetic complaints of bias, which offered a rare window into terrorist media criticism. TTP spokesman Ihsanullah Ihsan said his group would "continue to respect journalists" except for highly biased outlets. The spokesman for another Taliban insurgent group, Sirajuddin Ahmad of Maulana Fazlullah, spoke at greater length:

> He said media provided an opportunity to all those people who were opposed to the Taliban and their activities and used insulting language against them on media. "Right from UN Secretary General Ban Ki-moon to Hillary Clinton and President Obama, all of them used whatever bad language and words they could use on the media but when we tried to reply to them, no media organisation was willing to give us importance. The media is not even allowed to use the real name for Maulana Fazlullah but calling him derogatory names like Mulla Radio," Sirajuddin complained, but refused to admit that they planned attacks on the media.

Wow, Columbia Journalism Review, here we come. Clearly Pakistani reporters should be giving equal weight to the pros and cons of shooting children in the face.

The Taliban is mad because the rest of Pakistan is mad at them over the shooting. "Undoubtedly this is the worst press the TTP has ever had, there is no doubt," Rana Jawad, Islamabad bureau chief of Geo News, told The Guardian's Islamabad correspondent Jon Boone. The Taliban have been furious that justification for the attack, that the girl was being "un-Islamic," was not being placed prominently in news stories. Muhammad Amir Rana of the Pakistan Institute for Peace Studies, says the Taliban are taking a PR beating. "We have seen a similar public sentiment in the past, but this time it is quite unique," he said. "This case has provided a catharsis of the masses for all the grievances that have been building up for years."

Apparently, the insurgent groups just aren't very media savvy, according to Mullah Yahya, a former high-ranking Afghan Information Ministry official, who spoke with The Daily Beast's Sami Yousafzai. "First of all, attempting to kill a 14-year-old girl is a low act," he said. "Second, claiming responsibility for it is a sign that the [Pakistani] Taliban are not aware of the media's importance. I have seen more anger against the religious elements in the past week than in all my 40 years of life." So here's to you, Pakistani press. You've defied the all-too-common media trap of false equivalence.

Table of Contents

# Boeing Successfully Tests Microwave Missile That Takes Out Electronic Targets

From KMOX St. Louis, 25 Oct 2012

HILL AIR FORCE BASE, Utah (CBS St. Louis) — Boeing successfully tests a new missile that can take out electronic targets with little collateral damage.

The aerospace company tested the microwave missile last week on a two-story building on the Utah Test and Training Range where computers  and electronic systems were turned on to gauge the effects of the missile's radio waves, according to a Boeing press release.

The missile, known as CHAMP (Counter-electronics High-powered Advanced Missile Project), fired a burst of High Powered Microwaves at the building, successfully knocking out the electronic systems and computers, and even taking out the television cameras recording the test.

“This technology marks a new era in modern-day warfare,” Keith Coleman, CHAMP program manager for Boeing Phantom Works, said in the press release. “In the near future, this technology may be used to render an enemy’s electronic and data systems useless even before the first troops or aircraft arrive.”

Seven targets were taken out in total during the one-hour test which left no collateral damage.

Coleman believes this can be a huge advancement forward in non-lethal warfare.

“Today we turned science fiction into science fact,” Coleman said in the press release.

James Dodd, vice president of Advanced Boeing Military  Aircraft, is hoping to get these microwave missiles in the field sooner rather than later.

Members of the U.S. Air Force Research Laboratory Directed Energy Directorate and Raytheon Ktech also took part in the test.

Table of Contents

## Iran’s Global Cyber War-Room Is Secretly Hosted by Hizballah in Beirut

From DEBKAfile Exclusive Report October 21, 2012

Iran’s secret cyber war-room is located at Hizballah’s secret internal security apparatus headquarters in the Shiite Dahya district of South Beirut, debkafile’s exclusive intelligence and counterterrorism sources reveal. The hackers and cyber experts who recently attacked American banks and Saudi oil sites and which guided an Iranian stealth drone into Israeli airspace on Oct. 6, operate from Hizballah’s premises in Beirut and its secret bunkers.

Wafiq Safa is head of the security apparatus and also deputy of the Iranian general, Hossein Mahadavi, who serves as the liaison and coordination officer with Hizballah in Lebanon.Safa’s son is married to the Hizballah chief Hassan Nasrallah’s sister.

Cyber intelligence experts explain Tehran uses its Lebanese surrogate to host its global digital war-room - firstly, to disguise the source of its cyber offensives and keep Iran clear of blame; secondly, because the Hizballah facility is protected from electronic penetration by exceptionally efficient firewalls.

They were strong enough to keep Israeli cyber experts from discovering the electronic center which dispatched the UAV over their country and reaching its controllers.  Whenever Israel experts tried manipulating the drone’s movements, they found an external force overrode them and recovered control. Eventually, the Israeli commanders gave up and ordered the drone brought down with as little damage as possible.

The drone’s components have given up to its captors many secrets about Iran’s stealth UAV technology and capabilities, but very little about the Iranian cyber team operating out of the Hizballah facility in Beirut and their equipment.

By cutting away from the captured UAV, the Iranian controllers also locked their operation away from outside access and any possible evaluation of their capabilities.

The Americans encountered the same difficulty in early October when they tried to locate and identify the hackers who disabled 10 major US bank websites, attacked Saudi Arabia’s Aramco’s websites with a virus called Shamoon that replaced data with burning American flags, and invaded the computers of Qatar’s gas industry.

Six days after the drone’s penetration of Israel, US Defense Secretary Leon Panetta talked to reporters in New York about “a pre-9/11 moment” (http://www.debka.com/article/22438) for the United States. He did not come right out and name Iran or mention its cyber war headquarters in Beirut. He did, however, warn “the attackers are plotting,” and that recent electronic attacks in US and abroad demonstrate the need for “a more aggressive military role in defense and to retaliate against organized groups or hostile governments.”

Table of Contents

## After Snagging $4.6B Contract, Lockheed Plans ‘Cyber Kill Chain’ For Global Information Grid

By Debra Werner, Defense News, Oct. 22, 2012

SAN FRANCISCO — The Defense Department’s day-to-day operations are linked in a vast, international in-house data communications network called the Global Information Grid. Seven million people — uniformed members of the armed forces as well as civilians — rely on it to exchange classified and unclassified information on personnel, vehicles, weapons and surveillance systems. Now, in a coup coming in tight economic times, Lockheed Martin has taken over the multibillion-dollar contract to manage and upgrade the system.

One of the major innovations Lockheed plans to bring to the GIG is heightened cybersecurity, said Angela Heise, the company's vice president for enterprise information technology solutions. Hackers attempt to penetrate Defense Department computer networks millions of times per day, Defense Secretary Leon Panetta said Oct. 11 during a speech at the Intrepid Sea, Air and Space Museum in New York. Lockheed Martin plans to bolster the GIG's security with a "cyber kill chain" — a computer security measure aimed at what are called advanced persistent threats. In those attacks a hacker penetrates a network and remains there for months or even years. In order for that type of attack to succeed, hackers must worm their way into high-value networks, remain there undetected and send sensitive data to outside computers. Cyber kill chains seek to stop advanced persistent threats by blocking one or more of the hacker's steps.

The Defense Information Systems Agency stunned observers in June when it announced that Lockheed Martin Information Systems and Global Solutions won the GIG Services Management-Operations, or GSM-O, contract, worth as much as $4.6 billion over seven years, to manage the grid. It was a contract held for more than a decade by Science Applications International Corp.  SAIC protested the decision, claiming DISA failed to evaluate properly the risk and cost of Lockheed Martin's proposal. On Oct. 1, the General Accountability Office upheld the award, clearing the way for Lockheed Martin and its teammates to proceed.

DISA officials declined to discuss the controversy. Heise attributed Lockheed Martin's success to its plans to "transform" the network and a strong team that includes AT&T Inc., global aerospace giant BAE Systems; Telcordia Technologies Inc., the research and technology company formerly known as Bell Communications Labs; and Serco Inc., the U.S. arm of the British management services firm Serco Group PLC.

It will take Lockheed Martin and its partners six to nine months to take over managing the GIG and begin making improvements, Heise said Oct. 11. One of those innovations is an Amazon-powered storefront designed to help members of the armed forces, policymakers and support personnel find and purchase products and services related to the grid. Lockheed Martin also is seeking to improve database management.

"We have this large-scale global network and we need to be able to identify every element in that network: every router, every switch, every little piece along the lines," Heise said. "To be able to have a complete database of all that information is very significant not only for good management and operations, but it also helps us look for ways to transform that network."

On Oct. 2, DISA issued the first one-year task order to Lockheed Martin to take over day-to-day operations of the GIG, said DISA spokesman Steve Doub.

Loren Thompson, defense analyst with the Lexington Institute, said programs like GSM-O are particularly important to government contractors like Lockheed in light of looming federal budget cuts.

"GSM-O supplies essential support services to the military's global grid, and thus is the kind of award that is unlikely to be scaled back in a tight fiscal environment," Thompson said in an email. "If you were trying to build a stable federal information technology business in unstable times, this is the sort of contract you would want."

Table of Contents

## The Army Is Building Cyber into Its Combat Exercises

By John Reed, Foreign Policy, October 26, 2012

The Army has started incorporating cyber operations into exercises meant to prepare its heavy forces to fight major wars again after more than a decade of counterinsurgency, a three-star general revealed this week.

Until recently, "we had not thought through the process of how we could use cyber, or the network, from a weapons standpoint," said III Corps Commander, Lt. Gen. Donald Campbell during a speech at the Association of the U.S. Army's annual conference in Washington this week.

To address this, Campbell had representatives from U.S. Army Cyber Command embed with his commanders for the exercise, hosted by III Corps this summer, so that the traditional combat troops could learn how to use cyber in a conflict. (III Corps is a heavy combat formation of the U.S. Army consisting of numerous armor, cavalry and infantry divisions.)

"This was a Caspian Sea scenario against what I would classify as a near-peer adversary," said Campbell. This means that the friendly troops were fighting a nation with an advanced military, like Russia's.

In addition to throwing armor, artillery, and infantry at the enemy to defeat its forces, commanders got accustomed to thinking about how they would use cyber power in the campaign.

"I had to tell the staff, 'Here's what I want to achieve as an example,' as we got ready to isolate Baku, in really the culminating operation for the exercise. I specifically said I want to target this [enemy] division to do this to it -- not 'take it down', that's not a doctrinal term -- but to really impact its ability to command and control," said Campbell. "So we put together a [concept of operations] using [U.S. Army Cyber Command's] capabilities, [the Army cyber] team working to us to do that specific mission [taking out the enemy's command and control] and it was very successful."

What does very successful mean? The fake enemy's ability to command his forces and gather intelligence was degraded by about 40 percent because of Army cyber's efforts, according to Campbell.

"When [Army cyber commander Lt. Gen. Rhett Hernandez] talks about the network as a weapons system, in my opinion that was a great example," said Campbell.

He added that his operational planners had to learn how to collaborate with the cyber commanders to use cyber weapons.

"We met daily, in a targeting brief for an hour and there were specific focused targets on what we would do to the network and what we would do to our network," said Campbell.

Friendly forces even used social media in an attempt to win the local population's support.

"I asked the team to leverage what we could from a social media standpoint . . . to try to get after the populace," said Campbell, who added that this use of social media to influence the outcome of a conflict was "bigger than public affairs."

While the exercise was a start, the Army must make relationships between more traditional units like III Corps and its divisions and cyber forces "habitual," according to Campbell, who noted that several upcoming Army exercises will incorporate cyber.

All of this comes as the Army seeks to develop a new generation of cyber weapons and is working to incorporate offensive cyber fire support into its operations.

In addition to building strong and resilient networks capable of operating while under attack, "we must also be ready when directed to conduct offensive operations to help achieve commanders intents and the objectives that they desire," said Lt. Gen. Hernandez during the same event at which Campbell spoke.

Table of Contents

## Accolade for Troops' Community Radio

By Carla Prater, British Forces News, 25 October 2012

Full video report: click here

15 Psychological Operations Group have been awarded this year's Firmin Sword of Peace for their work in Afghanistan.

Over the last six years the unit has been building relations with the local community, and one of its main achievements has been setting up Radio Tamadoon across Helmand.

Radio Tamadoon was set up to support the community with weekly farming advice, a woman’s hour, poetry and music shows and its own radio drama, called Chai Dawat, or the Tea Shop.

The local community runs the station, but personnel from within Task Force Helmand support it.

The Firmin Sword of Peace is an accolade given to units for community and humanitarian work.

Table of Contents

## The Army Wants To Develop a New Generation of Cyber Weapons

By John Reed, Foreign Policy Killer Apps, October 23, 2012

The U.S. Army is conducting a new study to identify the cyber weapons it needs to develop, the service's top cyber officer said today.

"We're working hard with mission command as well as with [Army Space and Missile Defense Command] to work our way through an initial capabilities requirements document to determine what gaps we believe we have [in cyber and other elecronic weaponry]. . . to support tactical and operational requirements," said Lt. Gen. Rhett Hernandez, commander of Army Cyber Command during a speech at the Association of the U.S. Army's annual conference in Washington today.

Translated into English, that means that the service will look at the specific cyber effects that it needs on the battlefield (for example, taking over an enemy's communications networks or wreaking havoc on a base's power supplies) and it will then figure out the new weapons it needs to produce those effects.

This study "will produce a set of requirements that will drive an expanded level of capabilities beyond what we have today," added Hernandez.

These weapons could be in the form of more traditional electronic warfare (EW) tools such as those carried aboard aircraft or they could be advanced software weapons.

"As we identify those requirements that I think we see -- again, cyber or cyber related, whether you argue that it's EW or not -- it's part of that capability set that I think we'll be looking for and it's any capability that allows us to achieve it whether its airborne on the ground or others," said Hernandez in response to a reporter's question as to whether or not the service will look at airborne weapons.

Pentagon officials have traditionally been extremely tight-lipped about their offensive abilities in the cyber realm. However, this summer, Army and Marine Corps cyber officials acknowledged that they have conducted offensive cyber operations against the Taliban and that the services are developing ways for battlefield commanders to call for cyber fire support.

The Army is also developing a philosophy of "active defense" in cyberspace, much as the U.S. Air Force is doing. Active defense -- the tenets of which can border on offensive operations -- calls for defenders to snoop the networks of potential enemies and even hunt for hackers who are bent on attacking Army networks.

Also at the AUSA conference, Lt. Gen. Don Campbell, commander of III Corps, said the service and the nation as a whole must figure out rules of engagement for cyber weapons. "How far can we go to target this network or that network or capability or system, we're going to have to decide as a service or military," he said.

Hernandez did not say when the study will be done. Killer Apps has asked Army cyber for more information on this, we'll update when we hear back from them

Table of Contents

## Social Engineering & Cyber Security: What Military Leaders Should Take from Kevin Mitnick's Presentation

Blog – US Naval Institute, October 2012

Kevin Mitnick, the infamous hacker and social engineer turned security consultant, gave a presentation at this year's History Conference at the Naval Academy today. He gave numerous examples of extracting information from people and companies by using their own trust and knowledge against them. His demonstrations likely startled many of the audience members with the range of methodologies and, more importantly, the success rate.

Some may look at the seemingly endless list of ways attackers can obtain what they're looking for and throw their hands up in despair. It's important to take a step back and consider some important factors in responding to, and hopefully mitigating, attack vectors.

Technology alone won't save you. If you fight technology with technology, you'll lose. All the firewalls and intrusion detection systems in the world won't be a guarantee that networks won't be breached. There's no such thing as an impenetrable system, and no such thing as bugless software. Kevin's demonstration of exploiting vulnerabilities in widely used commercial software proves this. Moreover, this isn't just software being used in the private sector. Many of the exploits he demonstrated take advantage of software that's become an integral part of the way the military handles its information. As if this weren't enough, the files used to carry out every successful exploit passed antivirus scanning without incident, and were run on fully patched, up-to-date systems.

That's not to say technological security measures are pointless; far from it. Strong passwords, multi-factor authentication, limited access permissions, and strict data management are as important now as they've ever been. Placing full faith in their protection, however, is misguided.

Legislation and policy alone won't save you. The first instinct of most government and private agencies is to react to new threats with new rules. Congress will propose laws, companies will write new usage regulations, and in the end they'll do little to stem attacks. Punitive action will deter the low-level players for whom it isn't worth the risk of fines or prison, and employees will perhaps comply with increased restrictions on their behavior. Those with the determination and skill will get what they're seeking, and many of them won't be caught.

In fact, regulations have an unintended consequence: complacency. In an interview with news.usni.org Online Editor Sam Lagrone, Mitnick indicated that, as an example, PCI DSS gives corporations a checklist for protecting client financial data, allowing them to be in legal compliance and in so doing avoid large expense in comprehensive security. Companies will only spend as much money as is necessary, and regulations spell out that exact necessity, whether it's comprehensive or not. Companies feel secure in following the rules, and when the threat evolves beyond those rules the company lies vulnerable because they didn't remain vigilant. Similar risks exist inside military structures, where policies exist to restrict certain behaviors but can't account for new and inventive attacks, and result in training focusing in on symptoms rather than targeting the root problems.

Again, this isn't to say legislation is pointless. It is very useful in punishing those that are caught. It's also good incentive for organizations to take measures to protect data that they may otherwise be doing little to protect. Yet rules are inflexible, slow to change and expensive to enforce. The attacks against which they are designed to protect are anything but.

The military needs to take security training seriously. Anyone who's currently serving in the military or works for the Department of Defense has probably gone through basic computer security education, often consisting of nothing more than a one hour self-guided online course once a year. Nobody can reasonably deny that the military is effective in training its people in executing their missions – they train hard, they train continuously, and the result is a force for whom reacting to threats becomes instinct. Yet when it comes to protecting computer systems and preventing data leakage, it appears to be applied as more of an afterthought than a real training regimen. With nearly all the information the military handles stored digitally, every servicemember should be trained continually, and tested in their response to threats on a regular basis.

Kevin Mitnick proposed this type of approach as part of his presentation (typically given to corporate managers and executives), and this component of his talk is especially germane to military operations. It doesn't have to be significantly complex. Something as simple as an email intentionally crafted with inaccurate details that should throw up a red flag to trained users, and a link they're convinced to click (if they fall for the attack) that then informs them of their mistake. Something like a random phone call from a person posing as a superior and requesting details about a mission or personnel, and verifying that the proper procedures are taken for verifying identity or identifying a suspicious request. It would cost more money, but it's a crucial part of OPSEC and information assurance that isn't being given due consideration.

The bottom line: all hope is not lost. There's plenty that can be done to preserve military networks and defend against data leakage both from the outside and from the inside. The weakest part of any computer security strategy is always the user, and we should be putting more emphasis on doing everything we can to strengthen it.

Table of Contents

## Rogers Was Right, DOD-DHS Cyber Info Sharing Program Has Shrunk

Posted By John Reed, Foreign Policy, October 24, 2012

The joint DoD-DHS program that provides defense contractors with protection from bad cyber actors identified by U.S. intelligence agencies has actually shrunk, contrary to the Pentagon's earlier insistence otherwise.

The Defense Enhanced Cybersecurity Services (DECS) program has been touted as one way that the U.S. government can partner with private "critical infrastructure providers" to boost their online defenses. Under DECS, businesses pay their Internet service providers (ISPs) a fee to receive extra protection from specific threat signatures that have been identified by American spy agencies as being malicious. (Those signatures -- collected via secret means -- are given to the ISPs by the U.S. government.)

The program ran in pilot mode for nearly two years with 17 member companies subscribing, and it was opened up to a broader swath of companies last month.

However, several weeks ago, Rep. Mike Rogers (R-Mich.), chair of the House intelligence committee claimed that, while DECS is a good idea, the program has been shrinking, something the Pentagon denied. Until now.

"At the end of the operational pilot, one of the commercial service providers withdrew," a Pentagon spokesman explained in an Oct. 24 email. "During the operational testing of the pilot, five of the 17 DIB companies chose to withdraw and reallocate their resources to other corporate priorities."

That leaves 12 companies that are participating in the DECS program. Four of the five companies that quit during the pilot are considering rejoining a modified version of the program, according to DoD. These companies would cut out the ISPs as middlemen and receive threat signatures straight from the government, allowing them to monitor their own networks without paying the ISPs.

"Four of the five companies that withdrew are now reviewing the documentation for the permanent DECS component to determine whether to become an operational implementer, wherein they would be authorized to implement the services for their own networks," reads the email.

The Pentagon explained its earlier insistence that the DECS program still had 17 members by saying that since the program involves relationships between the defense contractors and ISPs, it did not receive updates on how many companies where actually participating.

"Under DECS, the services are primarily a relationship between the companies and their commercial service providers," reads the email. "Participating companies are not obligated to report data about their participation on a regular basis. When DoD responded to queries from the press on the number of companies that were participating in the program early last week, DoD used the best information available at the time. Subsequent further direct engagement with each company resulted in the more specific count above. To support House Permanent Select Committee on Intelligence (HPSCI) inquiries, DoD contacted each of the original 17 pilot participants for feedback and status."

Meanwhile, the larger initiative to which DECS belongs -- the Defense Industrial Base Cybersecurity Assurance (DIB CS/IA) program -- has been growing as advertised since it was opened to a large number of defense companies in May 2012, according to the Pentagon. DIB CS/IA allows for information-sharing about cyber threats between defense companies and the government.

"Since May 2012, the DIB CS/IA program has expanded from 34 to 65 companies, with new companies joining every week," read the spokesman's email. "In addition, since DoD recently finalized the processes for DIB CS/IA participants to join DECS, DoD continues to inform DIB companies of the availability of the services offered in the baseline DIB CS/IA program and the enhanced services under DECS."

Table of Contents

## Iranians Build up Afghan Clout

By Maria Abi-Habib, Wall Street Journal, 26 Oct 2012

HERAT, Afghanistan—Iran is funding aid projects and expanding intelligence networks across Afghanistan, moving to fill the void to be left by the U.S. withdrawal from Afghanistan by the end of 2014, according to U.S. and Afghan officials.

While Iran's spending here is nowhere near the billions the U.S. spends, Tehran's ability to run grass-roots programs and work directly with Afghans is giving its efforts disproportionate clout—something it could wield against American interests should the U.S. military strike Iran's nuclear program.

"Iran is the real influence here. With one snap of their fingers, they can mobilize 20,000 Afghans," said a high-ranking official in Afghanistan's presidential palace. "This is much more dangerous than the suicide bombers coming from Pakistan. At least you can see them and fight them. But you can't as easily see and fight Iran's political and cultural influence."

Many leading Afghan government officials have received Iranian support for years. President Hamid Karzai two years ago admitted that his office has regularly received suitcases of cash from Tehran, with as much as $1 million in euros stuffed inside, in exchange for "good relations."

Afghanistan is important to Tehran's efforts to break out of its international isolation as Iran's main regional ally, Syria, battles an insurgency. A pro-Iranian militant group in Lebanon, Hezbollah, has also been put on the defensive by the civil war in Syria, a Hezbollah benefactor.

Iran shares a language with many Afghans, about half of whom speak a dialect of Persian. Millions of Afghans work in Iran, and Iran is the main supplier of electricity to western Afghan cities like Herat, an hour's drive from the border. While Afghanistan is mainly Sunni Muslim, it has a large minority that shares Iran's Shiite branch of Islam.

Iran's main vehicle for spreading its influence across its eastern border is the Imam Khomeini Relief Committee, or IKRC, a secretive aid organization that operates around the world. The U.S. blacklisted IKRC's branch in Lebanon two years ago for aiding Hezbollah.

Unlike the U.S. Agency for International Development, which disburses its aid through private contractors and sometimes even hides the aid's American origin, the IKRC works directly with Afghan applicants, combining economic help with seeding efforts to gather intelligence, Western and Afghan officials say.

According to an Afghan man named Ali, who says he worked for IKRC vetting applicants for aid, they must supply extensive information on backgrounds and contact details of their extended family. U.S. officials believe IKRC uses the process to ensure aid goes only to those loyal to Iran.

Iran's embassy in Kabul and consulate in Herat didn't respond to requests for comment.

A senior U.S. official predicted Iran's efforts would fail because Afghans view them with suspicion. "The Afghans know who their true friends are," the official said, adding that the U.S. would have an enduring partnership with Kabul but Iran won't.

In Herat, IKRC provides loans to build houses; monthly stipends of oil, sugar, tea and medicine; and vocational courses. "As human beings, we will receive aid from whoever provides it," said Ali. "America is absent."

One recipient is Masooma Karimi. When she and her husband-to-be needed money for a wedding, IKRC paid for it and for furniture and kitchen goods.

The Iranians also paid for the wedding of Dunya and Saytaki Husseini, providing $400 and traditional clothes for the ceremony. "The Iranians are doing more than the Americans," said Mr. Husseini. "Iran is in all of our lives."

Ms. Karimi and the Husseinis live in the Herat neighborhood of Jubrayl, with many ethnic Hazaras who, like Iranians, are Shiites. Iran has built it a library, school, clinics and smooth roads—all Afghanistan rarities.

On a recent day in the library, a stack of books bearing a portrait of Iran's supreme leader, Ayatollah Ali Khamenei, was piled on the floor awaiting distribution to children.

The library doesn't just spread Iranian propaganda. Young girls use one room to learn English. There are classes in computer science and math.

"I would be happy if the U.S. would provide this aid, too, but they don't," said Reza, the manager, who uses just one name. "So I'm working with Iranian aid."

An employee, however, said the library had little choice: Officials from the Iranian consulate in Herat threatened to cut off funding this spring unless the library promoted more Iranian programs.

Another demand, the employee said, was to commemorate the June 3 anniversary of the death of Ayatollah Ruhollah Khomeini, leader of Iran's 1979 revolution. The library, needing the funds, agreed to increase its classes on Iranian culture.

"Soft power" isn't the only kind Iran projects. Herat provincial officials say they have seen a rise in insurgent activity by groups with Iranian backing. Insurgents "have safe houses in Iran and fight against the Afghan government," said Herat's governor, Daoud Saba.

In August, The Wall Street Journal reported that Iran had let the Taliban open an office in Iran and was increasing its support to the insurgency, aiming to speed up the U.S.-led coalition's withdrawal from Afghanistan.

Iran's President Mahmoud Ahmadinejad, at a meeting in China with Afghanistan's Mr. Karzai, said if the U.S. or Israel attacked Iranian sites, Iran would target U.S. Afghan bases, said officials who attended the meeting.

Western diplomats call Iran's moves partly a reaction to U.S. and European sanctions aimed at its nuclear ambitions, which have caused its currency to fall and inflation to rise. "They cannot attack Washington or London, but they can attack us," a senior Afghan official said.

Afghan officials say Iranian diplomats have long funded Afghan media outlets, and in August, officials in Iran's embassy in Kabul met with four Afghan TV stations and three newspapers in an effort to establish a union of Afghan journalists that would voice the Iranian line.

Afghanistan's intelligence agency struck back, arresting several Iranian journalists it claimed were Iranian spies. A Kabul-based reporter for Iran's semiofficial Fars News Agency remains in custody.

Mobarez Rashidi, Afghanistan's deputy minister of culture and information, acknowledged that the U.S.-led coalition, too, has funded the Afghan media to foster pro-American views. He drew a distinction. "We welcome countries that support media clearly and openly," he said.

Unlike the U.S., which focuses aid on restive provinces where the Taliban are strong, Iran empowers those that tend to be pro-Iranian.

Permission to enter Iran is potent tool. At Iranian-run clinics and mosques in Herat, when Afghans seek to enter Iran for medical care or a pilgrimage, only those deemed loyal to Iran get visas, said a senior Western official in Herat.

Herat's provincial health director felt Iran's wrath in 2008 when he sought to inspect an Iranian-funded clinic that was accused of giving patients pro-Iranian propaganda. The clinic, Sabz-e-Parsyan, is a gatekeeper for Afghans seeking treatment in Iran. The provincial official, Ghulam Sayed Rashed, says its staff refused to let him inspect the building fully.

He ordered the clinic shut until an inspection was completed, but two days later was overruled by a higher Herat official. The clinic's current director said he wasn't aware of the incident and denied any pro-Iran activity.

In any case, says Mr. Rashed, he and his family members have been denied visas to visit Iran ever since.

Table of Contents

## The Next Weapon of Mass Destruction Will Probably Be a Thumbdrive

Geoffrey Ingersoll, Business Insider, 29 Oct 2012

Despite congressional foot dragging, or maybe because of it, most defense and technology analysts are screaming dire warnings of impending cyber attacks, whether by Internet hacks or infected thumb drives.

Iran is ratcheting up "copy cat" cyber attacks on the U.S., and as per a report soon to be out, China has a vast military infrastructure set up to launch web-based attacks on foreign infrastructure. And that doesn't even factor in the 'lone wolf' Anonymous-type hackers who are just in it for the "Lulz."

Yes, folks, the Cyber War is going on right now, and it's a World War like nothing ever before seen.

Bill Gertz of the conservative-leaning Washington Free Beacon reports:

> The Project 2049 Institute, an Arlington, Va.-based think tank that focuses on Asian security issues, concluded that groups operating from Chinese territory have been “waging a coordinated cyber espionage campaign targeting U.S. government, industrial, and think tank computer networks.”

This "coordinated cyber espionage campaign" is waged from a new wing of the Chinese Military Industrial Complex called the "Beijing North Computing Center." Gertz goes on to say that analysts are calling this center another "department" since it's "similar to the United States National Security Agency, because of its signals intelligence work, its high-performance computing work, and its linguistic and code-breaking specialists."

And it's not just nation-states in the mix, civilian hacking groups from Russia and the Middle East (The Arab Electronic Army) are also targeting U.S. and foreign targets around the globe. Less vitriolic and militant, the hacktivist group Anonymous seems to target anybody whom they perceive to be blocking the "free flow of information" on the net.

The U.S. isn't standing down though — even if Congress won't pull the trigger on the cyber security bill, the military is leading the way in cyber deterrence and militarization. At the Air Force Academy there is training for permanent personnel wholly dedicated to fighting cyber wars.

Indeed, even the Marine Corps is getting in on the mix, in the hopes that they can weaponize cyber warfare to the point that it can supplement troops on the ground in small unit tactics.

Which brings the war full circle: as the military invests and Congress (grudgingly) forces infrastructure companies to update and harden networks, the most likely culprit in a cyber attack becomes the same culprit in the famous Stuxnet attack — a thumb drive.

Washington designed Stuxnet and then waited with bated breath for one of their on the ground 'assets' to slip it to an unsuspecting Iranian nuclear scientist.

From a report by Mashable:

> The answer turned out to be simpler than U.S. officials thought, since some plant personnel weren’t very careful with the thumb drives they were carrying. Thumb drives were “critical” in the initial Stuxnet attacks — which began in 2008 — although unspecified “more sophisticated” means were later used.
>
> “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand,” one of the program’s architects said.

If a network is hardened, and military redundancies, offensive as well as defensive, are put into place, then the next best option is a manual insertion, like with Stuxnet. In fact, it doesn't even need to be a thumb drive, it can be a phone or a PDA.

Recently, the National Security Agency has begun testing BYOD, or Bring Your Own Device, and hardening networks as cloud computing begins to take hold in defense agencies.

"It's very simple: 'I want one device.' I don't think it's any more complicated than that," Robert Carey, principal deputy CIO at the Department of Defense. Carey told TechWorld of the growing demand for BYOD policies. "Balancing ease of use and security is always the dynamic. Security is the antithesis of convenience."

What Carey is trying to say, is that there are gaping holes in security with regard to storage devices. Employees bringing in mobile devices is exactly where the Iranians went wrong in terms of Stuxnet.

More from the TechWorld report:

> Carey noted that the Pentagon is currently running multiple pilot programs to test various devices from other manufacturers, and working with vendors to harden mobile operating systems to meet DoD security requirements. But he held RIM, the maker of the BlackBerry, apart from other device makers for its focus on enterprise-grade security from the outset, while Apple, Android and other operating systems began with a consumer-centric approach, and have only been beefing up security in response to concerns from corporate and government customers.

"We have to manage this very carefully as we move into the future and make sure that these are not additional attack surfaces," Carey said to TechWorld. "I don't know that we'll quite get to a pure BYOD environment."

Soon, the weak networks of private American infrastructure companies will become hardened, if for any reason because the military's cyber skills toughen by the day — a quote from the Marines' "top cyber warrior," Lt. Gen. Richard Mills, on Aug. 15 about cyber warfare against the Taliban sums up America's future web defense:

> "I was able to get inside [enemy networks], and affect his command and control and, in fact, defend myself against his almost constant incursions to get inside my [cyber] wire to effect my operations," Mills said.

There are three rules of nationwide cyber security, laid out to us by Jarno Limnell, a cyber security expert:

1. — Resilience (defense): We must be able to withstand an attack.
2. — Attribution: We must be able to locate the attacker.
3. — Offense: We must be able to locate and destroy the attacker.

So the likelihood is that a terrorist action, a 'copy cat' terrorist action, by the Iranians, Chinese or anyone, would take place over a mobile digital storage device.

The reason for this is that it eliminates the last two rules: Iran suspected it was the U.S. and Israel who infected their nuclear sites, but didn't know for sure until the Obama administration leaked its responsibility.

Without knowing attribution, then you can't locate an enemy, and you can't launch an offense.

That's why the the next WMD won't be a suitcase bomb, it won't be chemicals wired to blow in Times Square, it'll be a well-placed thumb drive or a black berry which contains malicious code, placed by a homegrown terror agent, and brought in by an unwitting employee.

Table of Contents

## “Game Over” Text to Syrian Rebels – What’s the Message behind the Message?

Posted by Lawrence Dietz, PSYOP Regimental Blog, 28 Sep 2012

Imagine my surprise when I picked up local newspaper (the San Jose Mercury News) this morning and see the article “Syrian military's text to rebels: 'Game over'” (See: http://www.mercurynews.com/top-stories/ci_21648250/syrian-militarys-text-rebels-game-over). The same article appeared in a number of other publications such as the Boston Globe (see http://bostonglobe.com/news/nation/2012/09/27/syrian-military-text-rebels-game-over/GYGMyhAU8Drp0qf3qweWxM/story.html) (which is also the photo source).

The article describes a MISO campaign wherein the Syrian government has texted various rebels. The first reaction is that this is perhaps another one of those campaigns that I call the ‘surrender now and avoid the rush’ campaigns where the goal is to convince the enemy to surrender. The article makes it clear that the predominant feeling is that the campaign is not likely to influence any of the rebels to surrender or even diminish their activities. In fact the spike in rebel activity is partially attributed to the provocation of the text messages (see photo).

We can see that today’s battlefield is truly a 5 dimensional one (air, land, sea, space & cyber) as clearly expressed by the Economist (see http://www.economist.com/node/16478792). Just as the domains of war have blurred, it is important to remember that other aspects of the battlefield have evolved as well.

For example, the fact that the texts were delivered could also mean:  “we know who you are, we know where you are and because we control all communications, we are listening to every word you have to say.” It’s implied that SIGINT can be used to find the enemy and that the Syrian government can effectively deny the rebels their mobile phone communications.

While no one disputes the notion that the best defense is a good offense, it would be prudent for influence and kinetic warriors to consider the multi-level effects found on the 5th dimensional battlefield.

Table of Contents